REMARKS

Claims 29 - 43 are pending. Claims 1 - 28 have been cancelled. Claims 29 - 43 have been added. No new matter has been added. Applicant respectfully requests reconsideration of the application.

The Examiner objected to Figure 3 because Hash1 is mislabeled. The Applicants have amended Figure 3 to correctly identify Hash1 as illustrated in the enclosed red-lined and replacement copies.

The Examiner objected to the specification because the sections headings should not be underlined or boldfaced and should be in upper case lettering. The Applicants have amended the specification to place the section headings in upper case lettering.

The Examiner objected to claims 8 and 17 because of informalities. Claims 8 and 17 have been cancelled.

The Examiner objected to claims 6, 9, and 10 under 35 U.S.C. § 112, second paragraph, as having proper insufficient antecedent basis. Claims 6, 9, and 10 have been cancelled.

The Examiner rejected claims 1 - 10, 13, 16 - 18, 20, and 22 - 23 under 35 U.S.C. §103(a) as being unpatentable over U.S. Published Patent Application No. 2002/0178370 to Gurevich et al. ("the Gurevich reference") in view of U.S. Patent No. 5,604,801 to Dolan et al. ("the Dolan reference"). The Examiner rejected under 35 U.S.C. § 103(a) as being unpatentable over the Gurevich reference in view of the Dolan reference and further in view of U.S. Patent No. 5,418,854 to Kaufman et al. ("the Kaufman reference"). The Examiner rejected claims 21 and 24 are rejected under 35

U.S.C. § 103(a) as being unpatentable over the Gurevich reference in view of the Dolan reference and further in view of U.S. Patent No. 5,774,552 to Grimmer ("the Grimmer reference"). The Examiner rejected claims 25 - 28 under 35 U.S.C. §103(a) as being unpatentable over the Gurevich reference in view of the Kaufman reference. These rejections are respectfully traversed in so far as they are applicable to the currently pending claims.

Independent claim 29, recites:

> A method of generating a private encryption key, comprising:
> generating a public encryption key and a private encryption key in a client system;
> inputting a password and generating a random number;
> **creating a random private key by exclusive-ORing the private key with the random number;**
> generating a first hash value by hashing the password, a username, and a constant value;
> encrypting the random private key using the first hash value as an encryption key to create an encrypted random key;
> **generating a second hash value by hashing the password, the username, and a second constant value;** and
> **transmitting the username, the second hash value, and the encrypted random key to a server for storage.**

The Gurevich reference does not disclose, teach, or suggest the method of claim 29. The Gurevich reference is directed to a method and apparatus for secure authentication and sensitive data management. The Gurevich reference discloses having data that needs to be stored on a server. First, the sensitive data management utility (SDMU) program assigns an ID to the data item and generates a random number referred to as a server key part or SKP. Then, the SDMU constructs a key base by applying a special operation, e.g., a hash function to a combination of a token key, PIN, and the SKP. The key base is used to produce an encryption key for a symmetric encryption algorithm of choice. The data item is then encrypted with the created

encryption key. The encrypted data and the non-encrypted SKP and data item identification are transmitted to the server over a secure connection. The server entry creates a data entry in the database containing 1) a non-encrypted data item identification and a SKP and an encrypted data item content. *(Gurevich, page 6, paragraph 0068)*.

This is not the same as a method for generating and storing a private key including **creating a random private key by exclusive-ORing the private key with the random number.** The Gurevich reference never discloses the exclusive-ORing of a private key and a random number.

Further, this is not the same as a method for generating and storing a private key including **generating a second hash value by hashing the password, the username, and a second constant value;** and **transmitting the username, the second hash value, and the encrypted random private key to a server for storage**. The Gurevich reference does not disclose at all generating a second hash value. Also, the Gurevich reference discloses storing an encrypted data item, a non-encrypted data item identification and a SKP, e.g., the random number. This is not the same as a storing the username, the second hash value and the encrypted random private key because the Gurevich reference never generates a second hash value nor does it encrypt a random private key. Accordingly, applicants respectfully submit that claim 29 distinguishes over the Gurevich reference.

The Dolan reference does not make up for the deficiencies of the Gurevich reference. The Dolan reference discloses receiving a random number from the server. A hash value (H) of a message is created. The hash value (H) is exclusive-ORed with

KCARa (KCAR + H). The random number is exclusive-ORed with an encryption key (KEK1a + RNxa). (KEK1a + RNxa) is encrypted with (KCARa + H). The message and the encrypted value of (KEK1a + RNxa) are transmitted to the server. *(Dolan, Fig. 8; col. 8, line 47 - col. 9, line 5.)*.

This is not the same as a method for generating and storing a private key including **generating a second hash value by hashing the password, the username, and a second constant value;** and **transmitting the username, the second hash value, and the encrypted random private key to a server for storage**. The Dolan reference never discloses the generation of a second hash value utilizing the password, username and second constant value. Also, the Dolan reference transmits a message and an encrypted random key, but does not disclose transmitting the username nor the second hash value. Accordingly, applicants respectfully submit that claim 29 distinguishes over the Dolan reference, alone or in combination, with the Gurevich reference.

The Grimmer reference does not make up for the deficiencies of the Gurevich and the Dolan reference. Specifically, the Grimmer reference discloses the use of a one-way hash function on the user's name, password, and a random number and also the use of a second one-way hash function to be applied before transmission. Specifically, the Grimmer reference discloses, with protected simple authentication, that a user could append a random number to his user name and password. Before sending it to user 2, a one-way hash function is applied on that information, resulting in a protected token. The protected token is then transmitted to the second user, alone with the user's name, random number, and/or time stamp. The second user would then

query the directory to obtain user1's password, and then hash the copy of the password with the username, the random number, and/or time stamp. The second user would then compare the hash value with the protected token. The user1's identity would be confirmed if the results of this operation match the protected token. *(Grimmer, col. 4, line 57 - col. 5, line 7).*

This is not the same as a method for generating and storing a private key including **generating a second hash value by hashing the password, the username, and a second constant value;** and **transmitting the username, the second hash value, and the encrypted random private key to a server for storage.** While the Grimmer reference does disclose the generating of a second hash value, there is 1) no discussion of what exactly is hashed in the generation of the second hash value. Further, the Grimmer reference does not explicitly disclose what is transmitted to the server if a second hash value is created. For example, the second hash value could just be a hash of the first hash value. The Grimmer reference discloses only that a first hash value, a user's name, and a random number is transmitted to the server, which is not the same as transmitting a username, a second hash value, and an encrypted random private key. Further, there is a difference between a random number and a constant value. Accordingly, applicants respectfully submit that claim 29 distinguishes over the Grimmer reference, alone or in combination with the Gurevich and Dolan references.

The Kaufman reference does not make up for the deficiencies of the Gurevich reference, the Grimmer reference, and the Dolan reference. The Kaufman reference discloses that a workstation generates a random bit string and concatenates this to a

hash-coded version of the user password. The concatenated quantity is encrypted under the authentications server's public key and forwarded together with the username to the authentication server. The authentication server decrypts the message with its private key and checks that the workstation supplied the correct hash total for the user's password. If so, the server creates a ticket and performs an exclusive-OR on the ticket and the random bit string. This result is encrypted under the hash value of the user's password and returned as a message. *(Kaufman, col. 3, lines 28 - 48.)*

This is not the same as a method for generating and storing a private key including **generating a second hash value by hashing the password, the username, and a second constant value;** and **transmitting the username, the second hash value, and the encrypted random private key to a server for storage**. First, the Kaufman reference is hashing only the user's password and not three items (the password, the username, and the second constant value). Further, what is transmitted to the server is an encrypted value of a random number string concatenated with a hash value of a password, and a username. There is no second hash value transmitted nor is an encrypted random private key transmitted to the server. Accordingly, applicants respectfully submit that claim 29 distinguishes over the Kaufman reference in combination with the Gurevich, Dolan, and Grimmer references.

Independent claim 34 recites similar limitations to independent claim 29. Accordingly, applicants respectfully submit that independent claim 34 distinguishes over the Gurevich, Dolan, Grimmer, and Kaufman references, alone or in combination, for similar reasons as discussed above in regard to independent claim 29.

Claims 30 - 33 and 35 - 37 depend, directly or indirectly, on independent claims

29 and 34. Accordingly, applicants respectfully submit that claims 30 - 33 and 35 - 37 distinguish over the cited references for the same reasons as discussed above in regard to independent claims 29 and 34.

Independent claim 38 recites:

A method for retrieving a stored password, comprising:
receiving a password and a username;
generating a first hash value using the password, the username, and a first constant value;
generating a second hash value using the password, the username, and the second constant value;
transmitting the second hash value and the username to a key server; and
receiving an encrypted random private key from the key server if the username and the second hash value match a stored username value and a stored hash value.

The Gurevich reference does not disclose, teach, or suggest independent claim 38. The Gurevich reference discloses that a program sends to the server a data item identification that the server uses to locate the data entry for the item in the database. The server then transmits a server key part (SKP) and the encrypted data item back to the program. The SDMU program decrypts the data by utilizing the stored random number. *(Gurevich, page 6, paragraph [0070]).*

This is not the same as the method of claim 38. The Gurevich reference, in retrieving the encrypted data item, does not disclose **generating of a first hash value or a second hash value**. In addition, the Gurevich reference does not disclose **transmitting of the second hash value to the key server**. While the Gurevich reference discloses that if a data item identification matches, an encrypted data item and a stored item will be received, there is no disclosure of a comparison of both a username and the second hash value. Accordingly, applicants respectfully submit that

claim 38 distinguishes over the Gurevich reference.

The Dolan reference does not disclose the method of claim 38. The Dolan reference is directed to digitally signing a message and not to retrieving of a stored encryption key. Specifically, the Dolan reference discloses that a smart card sends a message to the server indicating that a message is to be signed and the server responds by sending a random number. The smart card generates a hash value H of the message and then exclusive-ORs the hash value H and an encryption key. The smart card exclusive-ORs a second encryption key and the random number and encrypts this total with the exclusive-OR value of the hash value H and the encryption key to create an encrypted value. The smart card transmits a request including a card ID, the encrypted value, and the message to the server. The server then regenerates the hash value of the message and exclusive-ORs the hash value and the first encryption key. Using this key, the server decrypts the encrypted value and recovers the user's secret key. The message is then signed using the secret key. *(Dolan, col. 8, line 39 - col. 9, line 24.)*

This is not the same as the method of claim 38. The Dolan reference does not disclose the **generating of hash values using passwords, usernames, and first and second constant values** because the Dolan reference only talks about generating a hash value of a message. The Dolan reference does not **disclose the transmitting of a hash value** because the Dolan reference discloses the transmitting of a message, an encrypted value, and a card ID. Further, the Dolan reference does not disclose the **receiving of an encrypted random private key** from the server after a comparison of a second hash value and a username to stored values of a hash value and username

are completed. Accordingly, applicants respectfully submit that claim 38 distinguishes over the Dolan reference, alone or in combination, with Gurevich reference.

The Grimmer reference does not make up for the deficiencies of the Gurevich and the Dolan references. The Grimmer reference discloses that a user1 would append a random number and/or time stamp to this name and password. User1 would apply a one-way hash function to the random number, the user name, and the password, which results in a protected token. The protected token is then transmitted along with the username, and random number to a second user. The second user queries a directory to obtain user1's password, and hashes that copy of the password with user1's name, the random number and/or time stamp just received, and compares the has value with the protected token. User1's identity is confirmed if the results match the protected token. A second one-way hash could be applied before transmission, but there is no disclosure of what values would be hashed. *(Grimmer, col. 4, line 57 - col. 5, line 8).*

This is not the same as the method of claim 38. Although there is a disclosure of a first hash value, there is no disclosure of generating a second hash value **utilizing the specific combination the username, the password, and a second constant value**. In other words, the Grimmer reference discloses that a second hash function could be performed, but there is no disclosure of what items or values are being hashed. Further, the Grimmer reference does not disclose a method including receiving an encrypted random private key from the key server if the username and the second hash value match a stored username value and a stored hash value. The Grimmer reference does not disclose that any value is received, and specifically does

not disclose that a random encrypted private key is received. Accordingly, claim 38 distinguishes over the Grimmer reference, alone or in combination, with the Gurevich and the Dolan references.

The Kaufman reference does not disclose, teach, or suggest the method of claim 38. The Kaufman reference discloses that a random number is generated, which is concatenated to a hash-coded version of the user's password. This quantity is encrypted under an authentication server's public key and forwarded, together with the username, as a message to an authentication server. The authentication server decrypts the message with its private key and checks that the workstation supplied the correct hash total for the user's password. If so, the server creates a ticket for the user and performs an exclusive-OR function on the ticket and the random bit string. The result of this is encrypted under the user's password hash value and returned as a message to the workstation. *(Kaufman, col. 3, lines 34 - 47).*

This is not the same as the method of claim 38. The Kaufman reference discloses only the hashing of a user's password, and not **the hashing of a username, a password, and either a first or second constant value**. The Kaufman reference does not disclose the transmitting of a second hash value, since it only talks about performing a first hash operation. Further, the Kaufman reference does not disclose the **receiving of a stored random encrypted private key if the second hash value and username are equal to stored values of the second hash value and username**. Instead, the Kaufman reference transmits back a value of an XOR of a created ticket and a random bit string which is encrypted with the user password's hash value. This value is created by the server by performing multiple operations, and is not

a stored random encryption private key. Accordingly, applicants respectfully submits that claim 38 distinguishes over the Kaufman reference, alone or in combination with the Gurevich, Dolan, and Grimmer references.

Independent claim 41 recites similar limitations to independent claim 38. Accordingly, applicants respectfully submit that claim 41 distinguishes over the cited references, alone or in combination, for similar reasons as discussed above in regard to independent claim 38.

Claims 39 - 40 and 42 - 43 depend, directly or indirectly, on independent claims 38 and 41. Accordingly, applicants respectfully submit that claims 39 - 40 and 42 - 43 further distinguish over the cited references for the same reasons as discussed above in regard to independent claims 38 and 41.

///

///

///

///

///

///

///

///

///

///

///

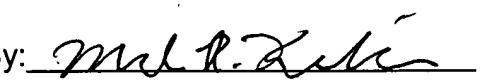
///

Applicants believe that the foregoing amendments place the application in condition for allowance, and a favorable action is respectfully requested. If for any reason the Examiner finds the application other than in condition for allowance, the Examiner is requested to call either of the undersigned attorneys at the Los Angeles telephone number (213) 488-7100 to discuss the steps necessary for placing the application in condition for allowance should the Examiner believe that such a telephone conference would advance prosecution of the application.

Respectfully submitted,

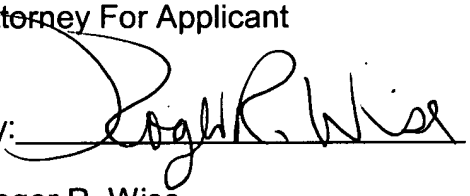
PILLSBURY WINTHROP LLP

Date: June 14, 2004

By: 

Mark R. Kendrick
Registration No. 48,468
Attorney For Applicant

Date: June 14, 2004

By: 

Roger R. Wise
Registration No. 31,204
Attorney For Applicant

725 South Figueroa Street, Suite 2800
Los Angeles, CA 90017-5406
Telephone: (213) 488-7100
Facsimile: (213) 629-1033